A FINANCIAL SYSTEM OF COMPUTERS

1   Background of the Invention:

2   This is a continuation of United States Patent application

3   serial number 09/166,749 filed on October 5, 1998, and entitled

4   "Financial System of Computers", now United States Patent number

5   5,963,917, issued on October 5, 1999, which was a continuation of

6   United States Patent application serial number 08/597,017,

7   entitled "An Improved Financial Transactions System" filed

8   February 5, 1996, now United States Patent number 5,822,737,

9   issued on October 13, 1998.

10   This invention relates generally to financial transactions

11 and more particularly to transactions involving credit or debit

12 cards.

13   The time is fast approaching where a significant amount of

14 commerce will be conducted using distributed networks of

15 computers such as the Internet. The reason this ground-swell of

16 commerce will occur is the ability of a single merchant to

17 economically reach a vast number of potential customers at

18 substantially no costs. Further, the customers are able to

19 review a great number of vendors and their products with the ease

20 of a few key strokes and clicks of the mouse.

21   Although there are vast numbers of merchants already using

1 such networks, the sales volume has been particularly low due to

2 a variety of reasons. One reason which has depressed commerce on

3 the networks, is the difficulty with which customers can pay for

4 their purchases.

5 A variety of techniques have been developed to cure this

6 problem ranging from accepting phone orders to the establishment

7 of another currency called "E-Cash".

8 Phone orders in response to merchant promotional materials

9 creates a variety of problems. One major problem is the

10 requirements for phone lines and personnel to receive and process

11 the phone orders. Another hurdle is the simple fact that most

12 customers have a single phone line to their residence and this

13 line is used by the computer for accessing the network; the

14 customer has to disconnect from the network to make the phone

15 order.

16 Although E-Cash is a viable alternative, it is faced with

17 some enormous problems which will be difficult or impossible to

18 address. These include: counterfeiting problems; government

19 reluctance to accept the concept; difficulties in getting access

20 for handling E-Cash; and, the low number of users and merchants

21 which can use E-Cash.

22 It is clear from the foregoing that there is a need for an

23 efficient methodology and system to accept payment over

24 distributed computer networks.

2

REPLACEMENT Amendment B

1   <u>Summary of the Invention:</u>

2   The present invention contemplates a totally automated

3   system for securing payment via a distributed network of

4   computers. In this context, the invention creates an automated

5   payment system particularly suited for purchases over a network

6   such as the Internet.

7   Although the present invention is described relative to the

8   Internet, its application is not so limited and is intended to be

9   used on any distributed computer system in which merchants and

10 consumers interact for the purpose of supplying and purchasing

11 goods or services.

12   In such a distributed computer network, a merchant or

13 vending computer contains certain promotional information which

14 is communicated to a customer's computer. This information is

15 intended to give the customer sufficient information to make a

16 decision on if the goods/services are acceptable.

17   As used within this discussion, the term "merchant computer"

18 signifies a computer system which is used for the purpose of

19 selling goods or services. The vendor itself does not

20 necessarily own the computer; in some situations, the computer is

21 operated on behalf of the merchant or vendor.

22   Based upon the promotional information, the

23 consumer/operator of the customer's computer decides to purchase

24 the services or goods described by the promotional information.

25   It is at this point where the present invention is

3

1 particularly powerful as it provides a simple, easy, methodology

2 and linkage for the customer to pay for the goods/services.

3   In this context, the customer's computer is linked to a

4 payment processing computer and the customer's credit card number

5 and the amount of the goods or services is transmitted to the

6 payment processing computer. For security reasons, an encrypting

7 software package is first downloaded to the customer's computer

8 so that the credit card number is secure from "hackers" who might

9 also be on the network.

10   Although the term "credit card" is used, the invention

11 covers the use of any type of financial guarantee card such as

12 automatic debit accounts, checking account numbers, savings

13 account numbers, and other such devices obvious to those of

14 ordinary skill in the art.

15   The payment processing computer automatically contacts a

16 bank for verification of the credit card and amount; the bank

17 transmits an authorization to the payment processing computer.

18 This authorization, usually in the form of a number, is stored

19 within the payment processing computer's memory for later

20 reference.

21   The link or connection with the bank is terminated by the

22 payment processing computer and the payment processing computer

23 turns its attention to the customer's computer. The payment

24 processing computer communicates a self-generated transaction

25 indicia, and in some embodiments a password, to the customer's

1 computer.

2 The transaction indicia is generated by the payment

3 processing computer for proper record keeping. The transaction

4 indicia is also used by the customer to verify that an order has

5 been generated and accepted.

6 The password is defined by the merchant's computer for the

7 payment processing computer to pass along to the customer's

8 computer. The password is used by the customer's computer to

9 gain access to restricted material within the merchant's

10 computer.

11 As example, assume the merchant's computer is supplying

12 information as to genealogy. As an initial process, the customer

13 enters the name being researched and receives a preliminary

14 report on the genealogy (the promotional material). To proceed

15 though, and get the actual data, the customer must pay to access

16 this further information.

17 To do so, the customer links with the payment processing

18 computer, and in the manner outlined above, receives back the

19 transaction indicia and the password. The payment processing

20 computer links the customer computer back to the merchant

21 computer; the customer provides the password to the merchant's

22 computer and is given access to the full genealogy report.

23 As outlined in this example, in the embodiment where a

24 password is used, the customer's computer uses the password with

25 the merchant's computer in obtaining access to protected

1   information or to establish shipping instructions.

2   The re-linking of the customer computer to the merchant

3   computer is accomplished in a variety of ways. In the preferred

4   embodiment, the payment processing computer obtains the

5   merchant's address or Unique Recognition Location (URL) from the

6   customer computer when the customer connects with the payment

7   processing computer. This URL is used in a variety of ways, to

8   identify the merchant, to establish the amount of the

9   product/service, and to establish the return URL when the payment

10   processing computer is done with its task for the customer

11   computer.

12   By selective use of the URL on the merchant's part, the URL

13   transmits a tremendous amount of information to the payment

14   processing computer. As example, assume the URL for the home-

15   page of the merchant is: merchant.com/widget.

16   When the merchant is selling a single product (a widget),

17   this URL is easy to match to the product. When the merchant

18   wants to sell a variety of widgets, then for a blue widget, the

19   URL might be: merchant.com/widget/blue.

20   In some embodiments, the customer's computer is not linked

21   back to the originating URL of the Merchant computer but rather

22   to another URL. The return URL is stored in the payment

23   processing computer and is used when the Merchant wants the

24   customer/consumer to be passed back to a different location (i.e.

25   where the restricted access information is accessible, or to

1   inform the consumer that their card has been rejected).

2   The invention, together with various embodiments thereof,

3   will be more fully explained by the accompanying drawings and the

4   following descriptions.

REPLACEMENT Amendment B

1   <u>Drawings in Brief:</u>

2   Figures 1A and 1B are block diagrams of the two computer

3   configurations used in the preferred embodiment.

4   Figure 1C is a graphical representation of the preferred

5   memory organization for the computer illustrated in figure 1A.

6   Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the

7   connections and disconnections of the preferred order.

8   Figures 3A, 3B, 3C, and 3D are frontal views of one

9   embodiment of a consumer's display screen.

10   Figure 4A is a flow-chart of the preferred embodiment's

11   payment processing operation.

12   Figure 4B is a flow-chart of an alternative embodiment's

13   payment processing operation.

14   Figure 5 is a flow-chart of the operation of the merchant's

15   computer.

1 <u>Drawings in Detail:</u>

2   Figures 1A and 1B are block diagrams of the two computer

3 configurations used in the preferred embodiment.

4   Figure 1A illustrates the configuration of the preferred

5 payment processing computer. As shown, computer 10A is a simple

6 layout of a Central-Processing-Unit (CPU) 11A which uses both

7 non-volatile memory 12A and Random-Access-Memory (RAM) 13A.

8   Communication to and from CPU 11A is via modem 14A which

9 communicates with other computers via the network connected by

10 phone line 15A.

11   Computer 10B, illustrated in figure 1B, shows the preferred

12 computer configuration used for the merchant computer and the

13 customer computer. Again, CPU 11B is connected to memories RAM

14 13B and non-volatile memory 12B. In the case of the merchant

15 computer, the promotional material is stored on non-volatile

16 memory 12B and is retrieved and communicated by CPU 11B using

17 modem 14B and phone line 15B.

18   This system is able to communicate with an operator via

19 monitor 16 for visual information. Monitor 16 is used for the

20 perusal of the promotional material by the customer.

21   Keyboard 17 is used to communicate operator commands to CPU

22 11B. In like fashion, mouse input device 18 is also used for

23 operator input to CPU 11B.

24   Optional printer 19 is used to create a hard copy of the

25 material being displayed to the operator/customer via monitor 16.

REPLACEMENT Amendment B

1   The differences between the computers shown in figure 1A and

2   1B are pronounce since the payment processing computer of figure

3   1A does not require input or direction from a human operator.

4   Rather, in the preferred embodiment, the payment processing

5   computer runs totally automatically and collects all of the data

6   and information it requires for its operation automatically from

7   the computers with which it is linked and with what is stored in

8   its memory.

9   Figure 1C is a graphical representation of the preferred

10   memory organization for the computer illustrated in figure 1A.

11   Memory 9, located preferably in non-volatile memory 12A, has

12   three sections. The first section 8A is the product listing

13   reference which is composed of multiple groupings. This data

14   remains relative constant and is defined by the merchant. Each

15   grouping, such as 7A, includes data identifying:

16   Part Number

17   Merchant Identification

18   Cost of Product/Service

19   Description of the Product/Service

20   Authorized Return URL

21   Rejected Return URL

22   Password

23   The second section is for defining the merchant's

24   information. Each grouping 7B within section 8B contains

25   relative constant information such as:

1   Merchant Identification

2   Business Name

3   Contact Name within the Business

4   Business Address

5   E-Mail address for the Business

6   Bank Checking Number for the Business

7   The third section 8C is an accounting listing which is

8 constantly up-graded as new payments are processed.   This section

9 is used for making full accounting to the various merchants.

10 Grouping 7C within section 8C contain:

11   Transaction Number

12   Date of transaction

13   Amount of the transaction

14   Part number involved in transaction

15   Credit Card Number

16   Authorization Number

17   The authorization number is the indicia received from the

18 bank indicating that the credit card charge has been accepted.

19   The use of memory 9 allows the payment processing computer

20 to have access to the necessary information to handle the linkage

21 and perform the proper accounting.

22   Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the

23 connections and disconnections of the preferred order.

24   Referring to figure 2A, in a typical fashion, a consumer via

25 customer computer 21 enters the network 20 and searches through

1   various merchant computers until the consumer locates the

2   merchant of choice and connects with merchant computer 22.

3   Merchant computer 22 communicates the promotional material via

4   network 20 to customer computer 21.

5   When the consumer decides to buy the service or product from

6   merchant 22, as shown in figure 2B, the link with merchant

7   computer 22 is broken and customer computer 21 links with the

8   payment processing computer 23. In the change from merchant

9   computer 22 to payment processing computer 23, an indicia of the

10 URL or the product being promoted by merchant computer 22 is

11 communicated to the payment processing computer 23.

12   The indicia as a URL of the last site is available through

13 normal network operations and its handling is obvious to those of

14 ordinary skill in the art. The product number is easily

15 combined with the URL; thereby making the product number also

16 available to the payment processing computer 23.

17   In some embodiments, the originating URL is crossed checked

18 to a memory data base to achieve the product number. In this

19 embodiment, the merchant structures its material so that only a

20 single product/service is associated with a specific URL.

21   Using the product number (or developing the product number

22 from the merchant's URL), the payment processing computer is able

23 to cross reference its own memory (as described earlier) to

24 achieve other important information including: the amount of the

25 product/service, a description of the product/service, the name

1   and address of the merchant, and other which will be used in

2   later operations.

3   The payment processing computer 23 accepts from the customer

4   computer 21, the credit card account number which is to be

5   debited the amount of the product.

6   As shown in figure 2C, in this embodiment, while maintaining

7   linkage with the customer computer 21, the payment processing

8   computer 23 establishes a link via phone lines 25 with the credit

9   card server computer 24. The credit card account number and

10   amount is communicated to the credit card server computer 24

11   which responds to the payment processing computer 23 with an

12   authorization indicia. This authorization indicia gives the

13   acceptance or denial of the charge.

14   If a product is to be shipped, and if the charge has been

15   authorized, as shown in figure 2D, the payment processing

16   computer 23 connects with the merchant computer 22 and directs

17   the merchant to ship the product to the consumer.

18   As shown in figure 2E, since the payment processing computer

19   23 has identified the product number, it is able to retrieve from

20   its memory the URL for reconnecting the customer computer 21 with

21   the merchant computer 22. In this manner, the entire operation

22   is totally transparent to the consumer since they feel they have

23   been continuously working with the merchant computer 22.

24   Further, using the URL's from its memory, the payment

25   processing computer 23 is able to link the customer computer 21

13

1 to the merchant computer 22 at an address which is different from

2 where the consumer was originally connected. In this manner, the

3 payment processing computer 23 is able to direct the consumer to

4 different locations which are consistent with the authorization

5 indicia (accept/reject) on their credit card.

6 As example, assume, the credit card was authorized, then the

7 consumer could be reconnected to an area which has restricted

8 access so that the consumer can gain the information paid for; if

9 on the other hand, the credit card was rejected, the connection

10 would be to a page indicating such and possibly asking for

11 another card number.

12 In this manner, the payment processing computer 23 is able

13 to control the operation and interface between the customer

14 computer 21 and the merchant computer 22.

15 Periodically, the payment processing computer 23 connects

16 via the phone lines 25 with the credit card server 24 and

17 instructs it to transfer the appropriate amount of funds to the

18 merchant's bank computer 26 so that the merchant has access to

19 the funds paid for his product/service provided to the consumer.

20 Figures 3A, 3B, 3C, and 3D are frontal views of one

21 embodiment of a consumer's display screen.

22 Screen 30A is designed to provide the promotional

23 information so that the consumer is attracted to purchase the

24 product. In screen 30A is the name of the merchant company (XYZ

25 CO.) 31, the name of the product (widget) 32, the price ($14.95)

14

1   33, and the part number (#10234) 34.

2   Also located on screen 30A is a software key 35 which allows

3   the consumer to pay for the product.   In this embodiment, by

4   activating this software key 35 (typically through a click of the

5   mouse), screen 30A is changed to screen 30B which is identical

6   except that the software key 35 has been replaced with an order

7   window 36.

8   Order window 36 allows the consumer to complete the

9   necessary information to order the product.   This includes the

10 part number 37A, the amount 37B, and the credit card number 37C.

11 When the consumer is ready, the software key "Send" 37D or the

12 software key "Cancel" 37E is activated.   In the case of a cancel,

13 the screen returns to screen 30A.

14   In a "send" 37D, mode, the payment processing computer

15 contacts the bank computer and determines if the credit card is

16 valid and if the amount is available.   If the charge is

17 authorized, the screen changes to 30C in which the order window

18 36 has been replaced with authorization window 38 which shows

19 that the charge has been accepted 39A, the transaction no.

20 (A1483) 39B, and the password ("GO") 39C which the consumer is to

21 use with the merchant.

22   When this information has either been printed or committed

23 to memory, the consumer activates software key 39D to "Proceed"

24 to screen 30D.   At this point, the consumer is able to enter the

25 password 29 so that the restricted access is lifted.   In the

1   genealogy example, it is at this point the consumer gains access

2   to the full report.

3   Figure 4A is a flow-chart of the preferred embodiment's

4   payment processing operation.

5   After start 40A, a connection is made with the customer

6   computer 41A and the encryption software is downloaded to the

7   customer computer 41B. Encryption software is preferably used

8   for transmittal of the credit card number so that the integrity

9   of the card is not jeopardized.

10   The consumer computer then communicates, and the payment

11 processing computer accepts, the account number, the amount, and

12 the identification of the product or service, 42A. A connection

13 is made with the credit card server 41C and the account number

14 and amount is transmitted 41D to the credit card server over the

15 established phone lines. In response to this query, the

16 authorization data is received 42B and the connection with the

17 credit card server 41E is broken.

18   A transaction indicia is generated 41F. This transaction

19 indicia is not the authorization data but serves as an internal

20 monitoring system for the payment processing computer so that the

21 accounting is kept accurate.

22   From the memory, the password is withdrawn 41G for the

23 product so ordered; and, the password and transaction indicia is

24 transmitted to the customer computer 41H.

25   At this point, the connection with the customer computer is

16

1   terminated 41I and the program stops 40B.

2   Figure 4B is a flow-chart of an alternative embodiment's

3   payment processing operation.

4   After start 43A, the program connects with the customer

5   computer 44A and at the same time obtains the merchant URL 45A.

6   Using the merchant URL, the payment processing computer searches

7   its memory and identifies the merchant number, the part number,

8   and the purchase amount 44B.

9   The encryption software is downloaded into the customer

10   computer 44C and the credit card account number is received 45.

11   A connection is then made with the credit card server computer

12   44D and the account number and the amount is transmitted 44E.

13   This inquiry results in an authorization code 45C being received

14   and the connection with the credit card server being broken 44F.

15   A check is then made to see if the credit card purchase was

16   authorized 46A.

17   If the credit card purchase was denied, the URL to use for a

18   rejection is withdrawn from memory 44G and the Customer computer

19   is connected to the merchant computer at this URL 44H leaving the

20   payment processing computer able to disconnect 44I and stop 43B.

21   Should the credit card purchase be accepted, 46A, then the

22   program generates a transaction identification 44J. This

23   transaction identification is stored along with the date, amount

24   of purchase, and the merchant number 44K.

25   The password is retrieved from memory 44L and it, together

1   with the transaction identification, is transmitted to the

2   customer computer 44M.

3   From memory, the authorized URL is withdrawn 44N.

4   A determination, based upon stored data, is made as to the

5   character of the product (service or goods) 46B. If the product

6   relates to goods which are to be shipped, a shipping order

7   including the transaction identification, the amount, the date,

8   and address of the customer, is communicated to the merchant 44O

9   to satisfy the order. If the product is a "service", the program

10   skips to step 44P.

11   The customer computer is then connected to the authorized

12   URL 44P and the connection with the customer computer is

13   terminated 44Q allowing the program to stop 43C.

14   Figure 5 is a flow-chart of the operation of the merchant's

15   computer.

16   After start 50A, the merchant computer connects with the

17   customer computer 51A and communicates the promotional material

18   52A. The password is received from the customer 52B and is

19   checked to see if it is the correct password 53A.

20   If the password is incorrect, a determination is made on if

21   it is the customer's first try 53B; if it is, then the customer

22   is given another chance to enter the correct password 52B. If

23   the customer has tried twice to enter the correct password, the

24   connection with the customer is terminated 51C and the program

25   stops 50C.

REPLACEMENT Amendment B

1   If the password is correct, 53A, then the secure or

2 restricted access data is communicated to the customer's computer

3 51D and the connection with the customer's computer is terminated

4 51B. The program then stops 50B.

5   In this manner, secure information is selectively

6 transmitted to a customer's computer upon the presentation of a

7 password.

8   It is clear from the foregoing that the present invention

9 creates a highly improved system for acceptance and processing of

10 payments over a distributed computer network.